UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,472	02/06/2006	Jan Camenisch	CH920020013US1	3674

54856 7590 05/27/2008

LOUIS PAUL HERZBERG
3 CLOVERDALE LANE
MONSEY, NY 10952

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/522,472	CAMENISCH ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 January 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/28/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of February 6, 2006. Claims (1-22) are pending and have been considered below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 4-6, 13, 16, and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Brennan et al. (US Patent No. 5,675,649 and Brennan hereinafter).

3. As to claim 4, Brennan teaches a **method comprising providing a signature value on a message in a network of connected computer nodes, the method being executable by a first computer node and the step of providing comprising the steps of:**

selecting (i.e., adding) **a first signature element** (e.g., signature) (i.e., Brennan teaches adding a signature to certificate information [col. 12, lines 29-31]);

selecting a signature exponent value from a number of exponent values (i.e., Brennan teaches (M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor [col. 10, lines 47-51]);

and deriving a second signature element from a provided secret cryptographic key, the message, and the number of exponent values such that the first signature element, the second signature element, and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key, where the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value, the signature value being sendable within the network to a second computer node for verification (i.e., Brennan teaches a third stage comprises creation of a self-signed certificate attesting the certificate authority name, public module N, and public exponent e and the validity period of these public key parameters. A secure hash function is applied to the certificate information to create a message digest, ext the message digest is encrypted with the certificate authority's secret key [col. 12, lines 22-30]).

4. As to claim 5, Brennan teaches a **method where the step of deriving a second signature element** (i.e., self-signed certificate) **further comprises deriving a signature base value using a provided public cryptographic key, the provided secret cryptographic key, and the exponent values** (i.e., Brennan teaches a creation of a self-signed certificate attesting to the certificate authority's name, public modulus N and public exponent e, and the validity period of these public key parameters. Brennan teaches a secure hash function is applied to the certificate information to create a message digest. Brennan teaches a next, the message digest is encrypted with the certificate authority's secret key, i.e. the message digest is signed by the certificate

authority. Brennan teaches a signature is then added to the certificate information to complete the certificate [col. 12, lines 20 – 32]).

5. As to claim 6, Brennan teaches a **method further comprising deriving a new secret cryptographic key from the provided secret cryptographic key and the selected signature exponent value** [col. 12, lines 20 – 32].

6. As to claim 13, Brennan teaches a **method further comprising applying each of the exponent values to at most one signature value** [col. 12, lines 20-32].

7. As to claim 16, Brennan teaches a **computer program element comprising program code means for performing the method, when said program is run on a computer (**i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

8. As to claim 17, Brennan teaches a **computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method** (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 1, 9-12, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brennan in view of Murakami (US Patent Publication No. 2001/0010721).

10. As to claim 1, Brennan discloses a **method comprising providing a secret cryptographic key and a public cryptographic key applicable in a network of connected computer nodes using a signature scheme, the method being executable by a first computer node and the step of providing comprising the steps of:**

generating the secret cryptographic key by selecting two random factor values (e.g., M and x) (i.e., Brennan teaches a secret parameters M and x, once generated provided a means of producing a cryptographically secure source of random numbers [col. 11, lines 60-63]),

multiplying the two selected random factor values to obtain a modulus value (i.e., Brennan teaches obtaining modulus value [N] [col.. 11, lines 64-67]), and **selecting a secret base value** (i.e., desired modulus size) **in dependence on the modulus value** (col. 11, lines 64-67), **where the secret base value forms part of the secret cryptographic key** (i.e., Brennan teaches a secret exponent d for which is used in forming the secret key [col. 12, lines 40-50];

generating the public cryptographic key by selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value (i.e., Brennan teaches a public key with exponent parameters [col. 12, lines 20-25]), **where the public base value and the modulus value form part of the public cryptographic key** (i.e., Brennan teaches a modulus and exponent value [col. 12, lines 20-25]);

and providing the public cryptographic key within the network; such that the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value (i.e., computationally infeasible) **on a message to be sent within the network to a second computer node for verification** (i.e., Brennan teaches M must be a large integer which is the product of two large primes p and q. It is recommended that M have the same number of bit its binary

expansion as does N. Absent specific knowledge of p or q. M must be presumed computationally infeasible to factor [col. 10, lines 47-51]).

However Brennan does not expressly teach:

deleting the two random factor values;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Brennan as introduced by Murakami. Murakami discloses:

deleting the two random factor values (to provide random value deletion capability [par. 50, lines 8-12])**;**

Therefore, given the teachings of Murakami, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Brennan by employing the well known features of random value deleting disclosed above by Murakami, for which secure generation of cryptographic keys will be enhanced [par. 50, lines 8-12].

11. As to claim 9, Brennan teaches a **method according to claim 1, further comprising applying each of the exponent values to at most one signature value** [col. 12, lines 20-32].

12. As to claim 10, Brennan teaches a **computer program element comprising program** (i.e., source) **code means for performing the method when said program**

is run on a computer (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

13. As to claim 11, Brennan teaches a **computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform the method** (i.e., function) (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

14. As to claim 12, Brennan teaches a **network device** (i.e., computer) **comprising: a computer program product** (i.e., code)**; a processor** (i.e., computer) **for executing the method; the processor** (i.e., computer) **having access to exchanged messages in the network** (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

15. As to claim 22, Brennan teaches a **computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing functions of a network device, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions** (i.e., Brennan teaches a computer used to execute source code to perform said functions [col. 4, lines 11-21]).

16. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brennan in view of Murakami as applied to claim 1 above, and further in view of Johnson (US Patent Publication No. 2001/0014153).

17. As to claim 2 and 3 the system disclose by Brennan in view of Murakami teaches substantial features of the claim invention (discussed above) it fails to disclose:

> **A method further comprising providing a description of the exponent values within the network (**claim 2).
>
> A **method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion** (claim 3).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Brennan in view of Murakami as introduced by Johnson. Johnson discloses:

> **A method further comprising providing a description of the exponent values within the network (**claim 2) (to provide exponent description capability within the network [par. 21, lines 10-14]).
>
> A **method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in**

the event of a detected intrusion (claim 3) (to provide exponent order to prevent exposure attack [par. 30 – par. 34]).

Therefore, given the teachings of Johnson, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Brennan in view of Murakami by employing the well known features of exponent description within a network disclosed above by Johnson, for which signature security will be enhanced [par. 21, lines 10-14].

18. Claims 7, 14, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chaum (US Patent No. 4,996,711) in view of Brennan.

19. As to claim 7, Chaum teaches a **method comprising verifying signature value on a message in a network of connected computer nodes, the method being executable by a second computer node and the step of verifying comprising the steps of:**

receiving the signature value from a first computer node (i.e., Chaum teaches a. receiving the signature value from a first computer node (This root is communicated to the second party's processor 1208 via a suitable communication link) [col. 20, lines 40-43); and;

and verifying whether the signature exponent value and part of the signature value satisfy a known relationship with the message and a provided public cryptographic key, otherwise refusing the signature value,

wherein the signature value was generated from a first signature element, a number of exponent values, a provided secret cryptographic key, and the message (i.e., Chaum teaches interval (the data processor means 1202 of a first party in conjunction with associated means 1204 is capable of determining an exponent from a first message using a procedure known to the first party and to a second party, the exponent containing at least one prime factor uniquely determined by the message. In addition, processor 1202 in conjunction with associated means 1206 is capable of forming a root on a constant known to both first and second parties, said root corresponding to the exponent. This root is communicated to the second party's processor 1208 via a suitable communication link (indicated by dotted lines in FIG. 12). Then processor 1208 in conjunction with associated means 1210 checks the received root by computing the exponent, raising the root to said exponent to produce a result and then verifying that the result is said constant) [col. 20, lines 31-46]).

However Chaum does not expressly teach:

deriving a signature exponent value from the signature value;

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Chaum as introduced by Brennan. Brennan discloses:

deriving a signature exponent value from the signature value (to provide exponent derivation capability [col. 11, lines 63-67]);

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Chaum by employing the well known features of exponent derivation disclosed above by Brennan, for which signature security will be enhanced [col. 11, lines 63-67].

20. As to claims 14, 18, and 19, the system disclose by Chaum teaches substantial features of the claim invention (discussed above) it fails to disclose.

A method further comprising applying each of the exponent values to at most one signature value (claim 14).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 18).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 19).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Chaum as introduced by Brennan. Brennan discloses:

A method further comprising applying each of the exponent values to at most one signature value (claim 14) (to provide exponent value for said signature [col. 12, lines 20 – 32]).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 18) (to provide code means for performing a method when said program is run on a computer [col. 4, lines 11-21]).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 19) (to provide computer readable program means for causing a computer to perform a method [col. 4, lines 11-21]).

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Chaum by employing the well known features of a computer readable program means for causing a computer to perform a method disclosed above by Brennan, for which secure generation of cryptographic keys will be enhanced [col. 4, lines 11-21].

21. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Staddon et al. (US Patent Publication No. 20040017916 and Staddon hereinafter).

22. As to claim 8, Johnson teaches a **method comprising communicating within a network of connected computer nodes the validity of a signature value in the event of an exposure of a secret cryptographic key relating to the signature value, the step of communicating comprising the steps of:**

defining an order of exponent values (par. 21, lines 1-10);

publishing a description of the exponent values and the order of the exponent values within the network (par. 21, lines 10-14);

, **the order of exponent values, and a provided public cryptographic key** (i.e., Johnson teaches a signature value comprising of a exponent, a key to determine validity of signature).

However Johnson does not expressly teach:

publishing a revocation reference to one of the exponent values within the network such that the validity of the signature value is determinable by using the revocation reference

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Johnson as introduced by Staddon. Staddon discloses:

publishing a revocation reference (i.e., revoke user are made public) **to one of the exponent values within the network such that the validity of the signature value is determinable by using the revocation reference** (to provide revocation notification of revoked parameters [par. 117, lines 4-8]).

Therefore, given the teachings of Staddon, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Johnson by employing the well known features of revocation notification disclosed above by Staddon, for which signature validation will be enhanced par. 117, lines 4-8].

23. Claims 15, 20, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Staddon as applied to claim 8 above, and further in view of Brennan.

24. As to claims 15, 20, and 21, the system disclose by Johnson in view of Staddon teaches substantial features of the claim invention (discussed above) it fails to disclose.

A method further comprising applying each of the exponent values to at most one signature value (claim 15).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 20).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 21).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Johnson in view of Staddon as introduced by Brennan. Brennan discloses:

A method further comprising applying each of the exponent values to at most one signature value (claim 15) (to provide exponent value for said signature [col. 12, lines 20 – 32]).

A computer program element comprising program code means for performing the method, when said program is run on a computer (claim 20) (to provide code means for performing a method when said program is run on a computer [col. 4, lines 11-21]).

A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method (claim 21) (to provide computer readable program means for causing a computer to perform a method [col. 4, lines 11-21]).

Therefore, given the teachings of Brennan, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of

modifying Johnson in view of Staddon by employing the well known features of a computer readable program means for causing a computer to perform a method disclosed above by Brennan, for which secure generation of cryptographic keys will be enhanced [col. 4, lines 11-21].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131